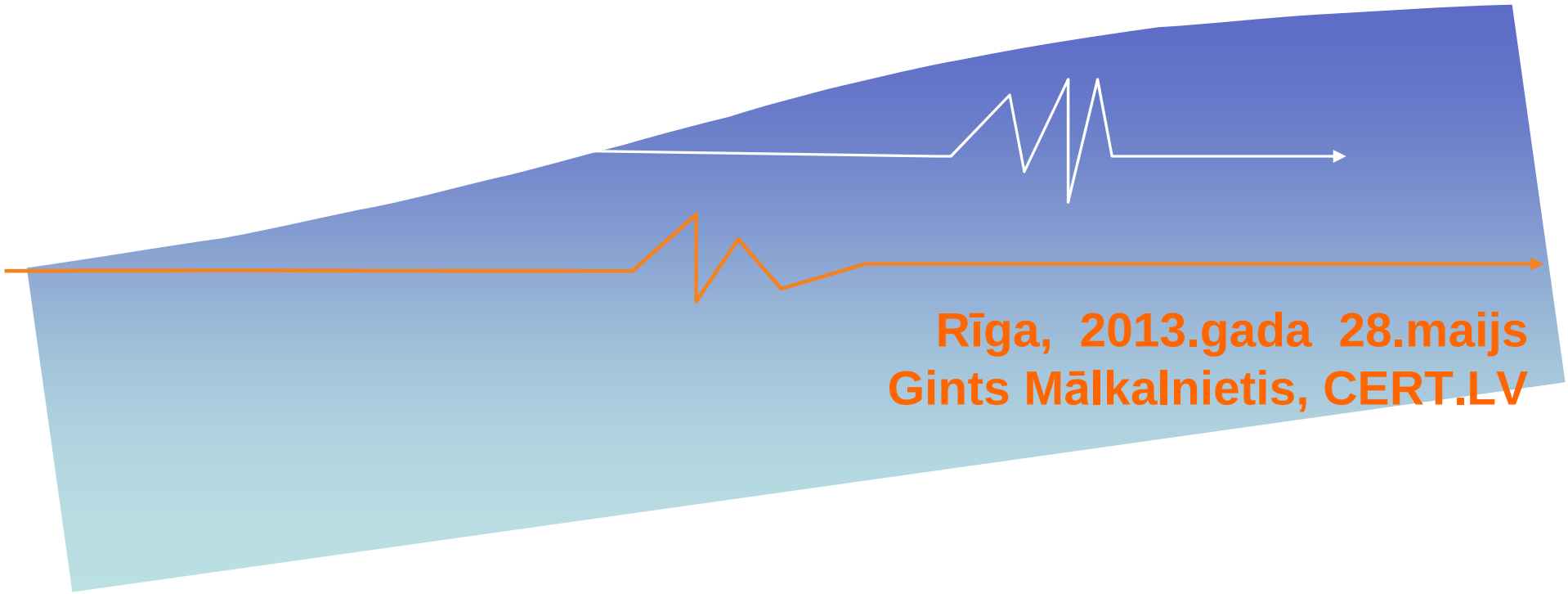
“Datorvīrusu ierobežošana”



Rīga, 2013.gada 28.maijs

Gints Mālkalnietis, CERT.LV

Saturs

- Kur slēpjas datorvīrusi
- Informācija datorvīrusa upurim

Kur slēpjas datorvīrusi?

1. Inficēts var būt JEBKURŠ dators!
   (arī Linux, BSD, Mac OS, iOS, Android)

2. Jāpārbauda ir VISI mājās esošie datori, kas tiek izmantoti

3. Jāpārbauda noņemamie datu nesēji:
   - ✓USB zibatmiņa
   - ✓Navigācijas iekārtas (TomTom, Garmin utt.)
   - ✓Citas iekārtas ar iebūvētu datu krātuvi – GSM modemi, mobilie telefoni, mūzikas atskaņotāji

Kur slēpjas datorvīrusi?

4. Tīkla iekārtas
   - ✓ novecojis programmnodrošinājums
   - ✓ nemainīta standarta parole
   - ✓ ieslēgti starpniekserveri
   - ✓ nozagta Wi-Fi parole
5. Biroja tehnika
   - ✓ Printeri – satur operētājsistēmu Windows 2000 vai Linux speciālas versijas
   - ✓ “Smart TV” – gandrīz pilnvērtīgs dators ar Linux OS
   - ✓ Dažādas specializētas mēriekārtas, medicīnas aparatūra

Kā atrast inficēto iekārtu

1. Izmantojot CERT.LV ziņojumā doto laika atzīmi konstatēt dotajā laikā aktīvo datoru.

   - ✓ CERT.LV ziņojumos laiks norādīts UTC laika zonā
   - ✓ Datoriem un tīkla iekārtām jābūt ar precīzi noregulētiem pulksteņiem (sinhronizācija no precīzā laika serveriem – vēlama)
   - ✓ Tīkla plūsmu (netflow) ieraksti ievērojami atvieglo inficētās iekārtas atrašanu
   - ✓ Intensīvi izmantotos tīklos vienlaicīgi ir aktīvi daudzi datori

Kā atrast inficēto iekārtu

2. Tīkla iekārtā (maršrutētājā) izveidot pārbaudes (audita) noteikumus, kas reģistrē pieslēgumus uz ziņojumā uzrādītajiem sensoriem.

- ✓ Ne visas tīkla iekārtas nodrošina šādas iespējas
- ✓ Lai atrastu DHCP piešķirtās adreses īpašnieku jāveic arī DHCP žurnalēšanu
- ✓ Sensoriem ir vairākas IP adreses, tās var dinamiski mainīties
- ✓ Labi jāpārzina sava tīkla maršrutētāju iespējas, un jāmāk tās izmantot
- ✓ Precīzs rezultāts, darbojas neatkarīgi no datora OS

Kā atrast inficēto iekārtu

3. Pārbaudīt visus tīklā esošos datorus
   - ✓ Lielos tīklos nepieciešams izmantot komandrindas rīkus un automatizācijas skriptus to izpildei
   - ✓ Aizņem daudz laika
   - ✓ Neder publiski pieejamiem Wi-Fi tīkliem

Ieteikumi mājas datora īpašniekam:

1. Pārbaudīt VISUS datorus ar antivīrusu CD
   - ✓ Esošā AV programma var būt novecojusi, vai arī vīrusa bojāta
   - ✓ Ne visas AV programmas ir vienlīdz efektīvas
   - ✓ Arī laptops ir dators (par viedtālruņiem, un planšetēm nemaz nerunājot)!

Ieteikumi mājas datora īpašniekam:

2. Pārliecināties ka Wi-Fi netiek izmantots nelegāli
   - ✓ Standarta paroles
   - ✓ Pārāk vienkāršas paroles (vēlams vismaz 14 simbolu garas)
   - ✓ Nedrošas šifrēšanas metodes izmantošana (WEP)

Ieteikumi mājas datora īpašniekam:

3. «Ciemiņu» datori
   - ✓ Legāli un nelegāli pieslēgumi tīklam
   - ✓ Draugu dators
   - ✓ Dators kas piepeši «sabojājies»

Dažas noderīgas adreses

Failu antivīrusu pārbaude- http://www.virustotal.com/
Pārlūkprogrammas drošības pārbaude - https://browsercheck.qualys.com/
Kaspersku Virus Removal- http://devbuilds.kaspersky-labs.com/devbuilds/AVPTool/
Bitdefender Rescue CD- http://kb.bitdefender.com/site/article/650/

Paldies!!!

Gints Mālkalnietis
E-pasts: gints@cert.lv
Tīmekļa vietne: http://www.cert.lv
Portāla Esi drošs tīmekļa vietne: http://www.esidross.lv
CERT.LV Twitter vietne: http://twitter.com/certlv